Spring 2-1-2019

CSCI 591.01M: ST - Database Security

Michael L. Martin
University of Montana, Missoula

Database Security

Faculty Contact

Michael Martin

Michael.martin@mso.umt.edu
martinml@ieee.org
360-622-5562
703-463-0915

Course Description

An overview of both the theory of and applications for providing effective security in database management systems. Topics include conceptual frameworks for discretionary and mandatory access control, data integrity, availability, secure database design, data aggregation and data inference. Models for multilevel secure databases for both relational and object-relational databases are analyzed. Assignments focus on database security concepts and require use of a remote access laboratory.

Course Outcomes

At the end of the course, students should be able to:

- Articulate database security techniques and procedures and use them to develop a database security plan
- Produce secure database designs
- Illustrate principles of discretionary and mandatory access control
- Recognize and apply availability concepts for security
- Assess different database security architectures
- Implement concepts of data integrity, data aggregation, and data inference in database secure environments
- Identify, define and distinguish between the fundamental issues in multilevel secure database systems
- Identify the common database threats and compile a list of counterthreats

Class Guidelines

Policy on Late Submissions:

The timely completion of all assignments is critical to student success. Take assignment deadlines seriously and allocate sufficient time to meet deadlines. Instructors may grant limited extensions for unexpected business, health, or personal emergencies beyond the student's control.
If you need an extension, make the request in advance of the assignment due date and support the request with a compelling rationale that is fair to the others in the class.

'Redoing' Assignments

There are assignments practically every week. Each week builds upon the next, and the assignments are chosen carefully to develop your skills and build your knowledge. It is important that you do a good job on all the assignments and that you turn them in on time. There is no extra credit granted in

this course, and you will not be able to redo assignments.

Submitting Original Work

You are encouraged to refer to and build upon the concepts, techniques, and ideas you have explored in previous coursework. However, everything you submit in this course must be original work written by you specifically for this course. Resubmission of coursework from a previous or concurrent course, partially or in its entirety, is unacceptable unless prior approval is obtained from the instructor for the specific assignment. Using coursework from a previous or concurrent course, partially or in its entirety, without explicit prior approval from your instructor will result in a grade of zero for the assignment.

Policy on Assignments (Online Classes)

All assignments are due at 11:59 pm on the last day of the session unless otherwise indicated. All individual and team assignments must be submitted in PDF, RTF, or Word format, as stipulated in the assignment description.

Course Specific Grading Policies

All work is required to be your original work. Late work without an extension granted in advance (before it is already late) -10% for late up to 1 week, -20% for over 1 week late up to two weeks late. Over two weeks late: No Credit. Make-up Work due at data as assigned by the instructor.

Homework Assignment:

The homework assignments are designed to provide practice translating security requirements to Oracle SQL and successfully implementing and testing that those requirements work as intended. The homework assignments are used as an indicator as to where everyone is in their understanding of the material necessary to do your project. All the homework assignments are geared towards giving you practice in something you must do for your project.

Participation:

You are expected to participate as necessary in the class. If there are discussion questions for the week you must post a response to at least one of them. If there is NOT a discussion questions you should not feel that you need to participate. You may not have a comment or questions for some of the sessions. If you have a question you should ask it! Students can answer each other questions (and are encouraged to do so). We often have some very experienced and knowledgeable students in the class. Most have not done much in Oracle security which is why you are taking the course. So, if you can answer another student's question about how to edit, maintain a spool file, where the spool files go, etc., please do so.

Project Descriptions

The lab project should be assembled in a format like a class paper. The main difference is that the subject is the student's own lab project and may not have many or even any references. Your name should be on the cover, pages should be number and the title of the project (and your name) should be on each page. It should be logically organized and professionally done (no spelling errors, clear writing).

Graduate Increment

There are 4 lab assignments in the course. The knowledge gained through successful

completion of the first two provided the knowledge necessary to complete the Lab project assignment: Graduate students are required to complete 2 additional labs assignment that cover advance security topics and require solid skills in programing functions typically gained in mastering a programming language. Graduate students are also required to use one or both advance techniques in their Lab Project. Undergraduates may complete either or both additional labs for extra credit.

Graded Work Assignments

Assignment	Frequency	Level of Effort	Percent of Grade	Comments
Discussion Topics	**1-3 per week; must do 1**	**2-3 Paragraphs**	**10**	**Take home**
Lab Assignment	**2-4 per semester**	**3-5 pages**	**10 U – 20 G**	**Take home**
Midterm	**1**	**4-8 pages**	**25 U – 20 G**	**Take home**
Lab Project	**1**	**15-30 pages**	**30**	**Take home**
Final	**1**	**4-8 pages**	**25 U –20 G**	**Take home**

Class Schedule

1) Jan 10-13: Database Security (Course Overview)

- Information Security
- Evolution of Security
- Review of Database Concepts
- Security Problems in Databases
- Threats & Security Controls

2) Jan 14-20: Introduction to Structured Query Language (SQL)

- Installing Oracle 12C
- Query Statements
- Data Manipulation Language
- Data Definition Language
- Data control Language
- Using SQL Plus
- Select Statement
- Creating a User
- Creating a Table
- Modifying a Table (Insert, Update, & Delete)
- Lab 1 Introduced: Due Feb 3

3) Jan 21-27: Security Policy, Plans, Procedures & Models; and Security Authentication

- Security Policy, Plans, Procedures, & Models
- Authorization Systems Integrity
- Harrison- Ruzzo-Ullman Take-Grant Model
- Access Matrix Mode
- Capabilities Lists

4) **Jan 28-Feb 3: Data Access Control & Security Models**

- Bell-LaPadula Model
- Biba Model
- Jajodia/Sandhu Model
- Clark Wilson Model
- Chinese Wall Model
- Sea View Model
- Developing Security Plans & Measuring Risk
- Role Based Access Control

5) Feb 4-10: Identification & Privilege Restriction

- Oracle Password Management
- Default Oracle Users
- External & Remote User
- Identification
- Privileges, Grants, Roles, and Views
- Controlling User Access & Granting Privileges
- Use of Roles, Views, & Triggers
- Authentication
- SQL
    - Users, Privileges & Roles
    - Views
    - Joins
- Lab 2 Introduced: Due Feb 17

6) Feb 11-17: Virtual Private Databases - Definition & Foundations

- Introduction to VPDs
- How VPDs work
- VPD Components
- How to use VPD
- Example
- Security Measures
- Direct Attacks Against Computer

7) Feb 18-24: Midterm

- Midterm Introduced Feb 18: Due Feb 24

8) Feb 25-Mar 3: Virtual Private Databases – Implementation Example

- Row-Level Security
- Column -Level Security
- Lab 3 Introduced Feb 25: Due Mar 10

9) Mar 4-10: Oracle Label Security - Features in Systems Oracle Label

- Security Policy
- Security Levels
- Security Components
- Security Data Labels
- Administering User Labels
- Setting Security Level,
- Components,
- and Groups
- Setting User Labels

10) Mar 11-17: Oracle Label Security – Continued

- Choosing Policy Options
- Label Management Enforcement
- Applying Policies to Tables (&
- Schemas)
- Viewing Session Label
- and Row Label
- Oracle Label Security
- Data Dictionary
- Tables and Views
- Restrictions in
- Oracle Label
- Lab 4 Introduced: Due Mar 24

11) Mar 18-24: Oracle Label Security – Example

- Example of OLS – Applied

12) Mar 25-31: Spring Break

13) Apr 1-7: Database Links

- Oracle Database Links
- Security Problems with Database Links
- Shared, Global, & Private Links
- Database Links Fine-Grained
- Access Control & Application Context

14) Apr 8-14: Advanced & Additional Topics

- Invoker & Defender Rights
- Intrusion Detection

15) Apr 15-21: Denial of Service Attacks

- Operating Systems Concepts
- Cross Site Scripting

16) Apr 22-28: Special topics

- Special Topics
- Project due Apr 28

17) Apr 29-May 3

- **Final**